RSA SecurID Ready Implementation Guide

Last Modified: September 30, 2005

Partner Information

Product Information	
Partner Name	Cisco
Web Site	www.cisco.com
Product Name	Cisco PIX Security Appliance
Version & Platform	PIX IOS 7.0(2)
Product Description	The market-leading Cisco PIX Security Appliance Series delivers robust user and application policy enforcement, mutlivector attack protection, and secure connectivity services in cost-effective, easy-to-deploy solutions. These purpose-built appliances provide multiple integrated security and networking services. Ranging from compact, plug-and-play desktop appliances for small and home offices to modular gigabit appliances with superior investment protection for enterprise and service-provider environments, Cisco PIX Security Appliances provide comprehensive security, performance, and reliability for network environments of all sizes.
Product Category	Perimeter Defense (Firewalls, VPNs & Intrusion Detection)

Solution Summary

The Cisco PIX® Security Appliance Series delivers robust user and application policy enforcement, multi-vector attack protection, and secure connectivity services in cost-effective, easy-to-deploy solutions. The Cisco PIX® Security Appliance Series provides convenient methods for authenticating VPN users through native integration with popular authentication services, including RADIUS and RSA SecurID authentication (without requiring a separate RADIUS/TACACS+ server to act as an intermediary).

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication, or RADIUS,
List Library Version Used	Library Version # 5.0.3
RSA Authentication Manager Name Locking	Yes
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	Yes (hardware dependent for number of servers)
Location of Node Secret on Agent	In flash
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	Designated Users, All Users, Default Method
RSA SecurID Protection of Administrative Users	No
RSA Software Token API Integration	Yes
Use of Cached Domain Credentials	No

Product Requirements

Partner Product Requirements: Cisco PIX Security Appliance	
Memory	See Cisco PIX Security Appliance documentation
Firmware Version	7.0(2)

Additional Software Requirements	
Application	**Additional Patches**
Cisco Secure VPN Client	4.6

! Important: If you are configuring the PIX Security Appliance to use IPSec you will also need to configure the Cisco VPN client. Information on how to configure the Cisco VPN client can be found in the Cisco VPN client implementation guide located at:

http://rsasecurity.agora.com/rsasecured/guides/imp_pdfs/Cisco_VPN_Client_AuthMan61.pdf .

Agent Host Configuration

To facilitate communication between the Cisco PIX Security Appliance and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database and RADIUS Server database if using RADIUS. The Agent Host record identifies the Cisco PIX Security Appliance within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces
- RADIUS Secret (When using RADIUS Authentication Protocol)

When adding the Agent Host Record, you should configure the Cisco PIX Security Appliance as a Communication Server. This setting is used by the RSA Authentication Manager to determine how communication with the Cisco PIX Security Appliance will occur.

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host records.

Partner Authentication Agent Configuration

Before You Begin

This section provides instructions for integrating the partners' product with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Cisco PIX Security Appliance

Log onto the Cisco PIX Security Appliance and enter enable mode, by typing the word "enable" and giving the enable password. Then enter configuration mode by typing "config t". You are now able to enter the commands below to turn on authentication.

VPN Configuration

Please refer to the following Implementation Guide for instructions on setting up the Cisco VPN client to use with the VPN configuration section.

http://rsasecurity.agora.com/rsasecured/guides/imp_pdfs/Cisco_VPN_Client_AuthMan61.pdf

RSA Native SecurID authentication configuration:

Note: The PIX Security appliance obtains the Authentication Manager's server list when the first user authenticates, which can be either the primary or a replica. Defining replica servers is not necessary when configuring Native Support.

RSA Authentication Manager:

```
aaa-server AuthMan6 protocol sdi
 reactivation-mode timed
aaa-server AuthMan6 host 10.100.50.37
 retry-interval 3
 timeout 13
```

VPN Policy:

```
ip local pool test 173.16.16.1-173.16.16.254

crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside


isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 2


tunnel-group AuthMan6Group type ipsec-ra
tunnel-group AuthMan6Group general-attributes
```

```
 address-pool test
 authentication-server-group AuthMan6
tunnel-group AuthMan6Group ipsec-attributes
 pre-shared-key *
```

RADIUS authentication configuration:

RADIUS Server:

```
aaa-server inauth protocol radius
aaa-server inauth host 10.100.50.37
 key secret
aaa-server inauth host 10.100.50.36
 key secret
aaa-server inauth host 10.100.50.35
 key secret
```

VPN Policy:

```
ip local pool test 173.16.16.1-173.16.16.254

group-policy ScottRAD internal
group-policy ScottRAD attributes

crypto ipsec transform-set RADIUSset esp-3des esp-sha-hmac
crypto dynamic-map RADIUSmap 30 set transform-set RADIUSset
crypto map newmap 30 ipsec-isakmp dynamic RADIUSmap

crypto map newmap interface outside
isakmp enable outside
isakmp policy 30 authentication pre-share
isakmp policy 30 encryption 3des
isakmp policy 30 hash sha
isakmp policy 30 group 2
isakmp policy 30 lifetime 86400

tunnel-group ScottRAD type ipsec-ra
tunnel-group ScottRAD general-attributes
 address-pool test
 authentication-server-group inauth
 default-group-policy ScottRAD
tunnel-group ScottRAD ipsec-attributes
 pre-shared-key *
 trust-point torque
```

Firewall Configuration

```
aaa-server partner-auth protocol radius
aaa-server partner-auth (inside) host 10.100.50.37 sharedsecret timeout 30
aaa authentication include ftp outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 partner-
auth
aaa authentication include http outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
partner-auth
aaa authentication include telnet outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
partner-auth
```

Note: You can also enter the word “any” in place of the service, ftp, telnet, etc, to have all services use authentication.

Certification Checklist: Firewall

Date Tested: September 29, 2005

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1	Windows 2003
RSA Software Token	3.0.4	Windows 2000
Cisco Pix Security Appliance	7.0(2)	IOS

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	N/A	Force Authentication After New PIN	✓
System Generated PIN	N/A	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	N/A	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	N/A	User Defined (5-7 Numeric)	✓
User Selectable	N/A	User Selectable	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
PASSCODE			
16 Digit PASSCODE	N/A	16 Digit PASSCODE	✓
4 Digit Password	N/A	4 Digit Password	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
Name Locking Enabled	N/A	Name Locking Enabled	▨
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓
Additional Functionality			
RSA Software Token API Functionality			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
Domain Credential Functionality			
Determine Cached Credential State	N/A	Determine Cached Credential State	▨
Set Domain Credential	N/A	Set Domain Credential	▨
Retrieve Domain Credential	N/A	Retrieve Domain Credential	▨

BSD/SWA ✓ = Pass ✗ = Fail N/A = Non-Available Function

Certification Checklist: VPN

Date Tested: September 29, 2005

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1	Windows 2003
RSA Software Token	3.0.4	Windows 2000
Cisco Pix Security Appliance	7.0(2)	IOS
Cisco VPN Client	4.6	Windows 2000

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	✓	Force Authentication After New PIN	✓
System Generated PIN	✓	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	✓	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	✓
User Selectable	✓	User Selectable	✓
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	✓
PASSCODE			
16 Digit PASSCODE	✓	16 Digit PASSCODE	✓
4 Digit Password	✓	4 Digit Password	✓
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	✓
Name Locking Enabled	✓	Name Locking Enabled	
No RSA Authentication Manager	✓	No RSA Authentication Manager	✓
Additional Functionality			
RSA Software Token API Functionality			
System Generated PIN	✓	System Generated PIN	✓
User Defined (8 Digit Numeric)	✓	User Defined (8 Digit Numeric)	✓
User Selectable	✓	User Selectable	✓
Next Tokencode Mode	✓	Next Tokencode Mode	✓
Domain Credential Functionality			
Determine Cached Credential State	N/A	Determine Cached Credential State	
Set Domain Credential	N/A	Set Domain Credential	
Retrieve Domain Credential	N/A	Retrieve Domain Credential	

BSD/SWA

✓ = Pass ✗ = Fail N/A = Non-Available Function

Known Issues

1. **Failed PIN creation via RADIUS with VPN Client.** When a user fails to enter a PIN that matches the PIN criteria they will be prompted to enter their password again but will always fail as the information the user enters will not be sent to the RADIUS Server. The user needs to disconnect and reconnect to attempt to create the PIN again.

Appendix

Node Secret: The Node Secret file is stored in flash on the Cisco PIX Security Appliance. To see this file run `show flash`. The Node Secret file will be named with the IP Address of the Primary RSA Authentication Server with a .sdi extension. Example 10-10-10-2.sdi